Evolution of Distributed Denial of Service Attacks on the Internet: Since 1994 up to the Present

Edgar Mikayelyan, Qrator Labs

++ HighLoad Armenia

Co-organizer

Yandex

Driving Forces of the Attack Evolution

Channel capacity

Processing speed

Generation and amplification capabilities

Possibility of protection

Credit: Icons made from http://www.onlinewebfonts.com/icon is licensed by CC BY 3.0

Driving Forces of the Attack Evolution

Channel capacity

Processing speed

Generation and amplification capabilities

Possibility of protection

RFC

New protocols implementation mechanisms

Credit: Icons made from http://www.onlinewebfonts.com/icon is licensed by CC BY 3.0

Dynamics of Driving Factors

x~10^6
100Mbps..100Tbps
edge capacity

x~100 10M..1G hosts
x~10^6 1Kbps..1Gbps в
home/office

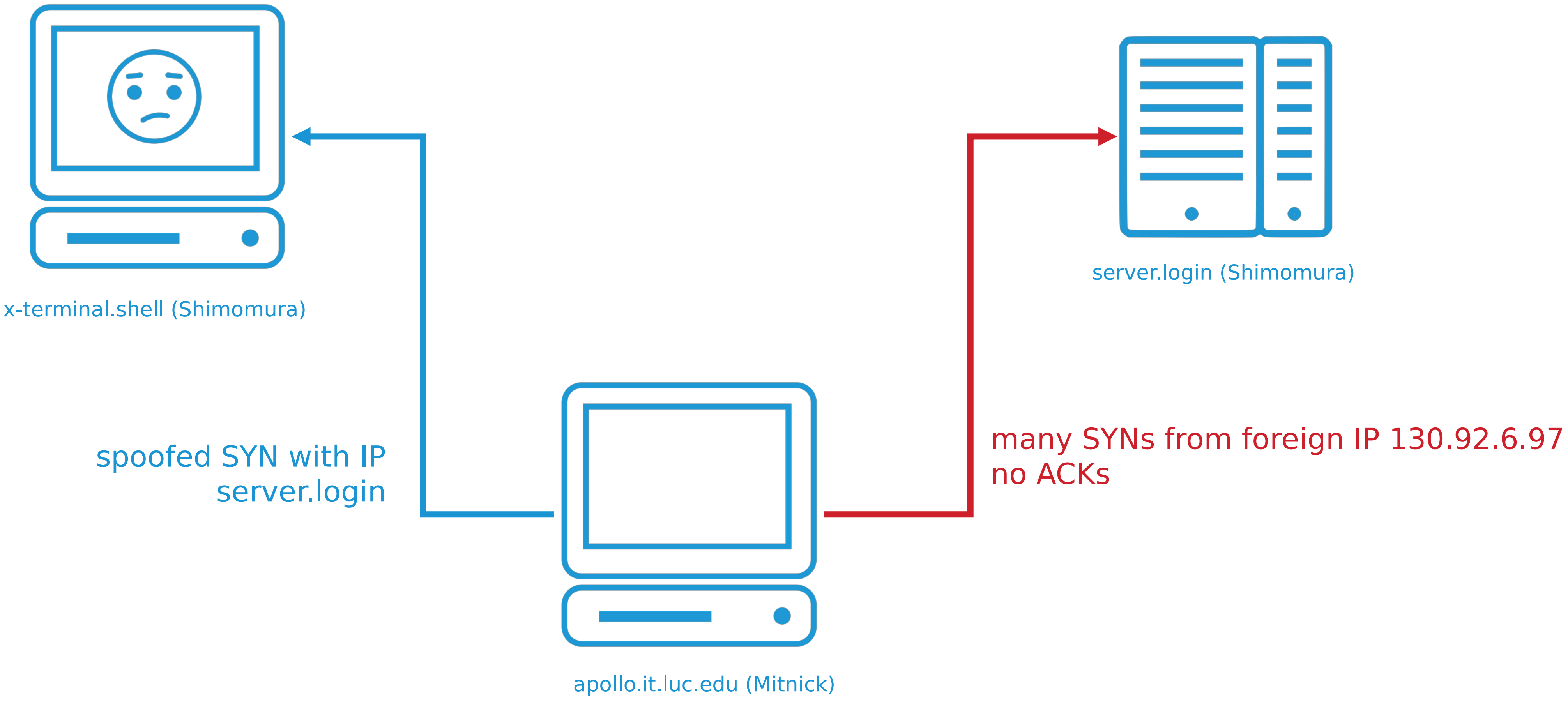
x~10^4
Kpps..10Mpps
on router

x~100 CPE bandwidth
x~1000 Cloud antiDDoS
bandwidth

Pacific Bell AN ‘1996..Hurricane Electric ‘2022
Cisco 2500 ’1996..Cisco ASR 1000 ‘2022
Data: Internet Systems Consortium 1997-2019+
Arbor PeakFlow **’2006..Arbor TMS ‘2022,** Qrator Labs 2010..now

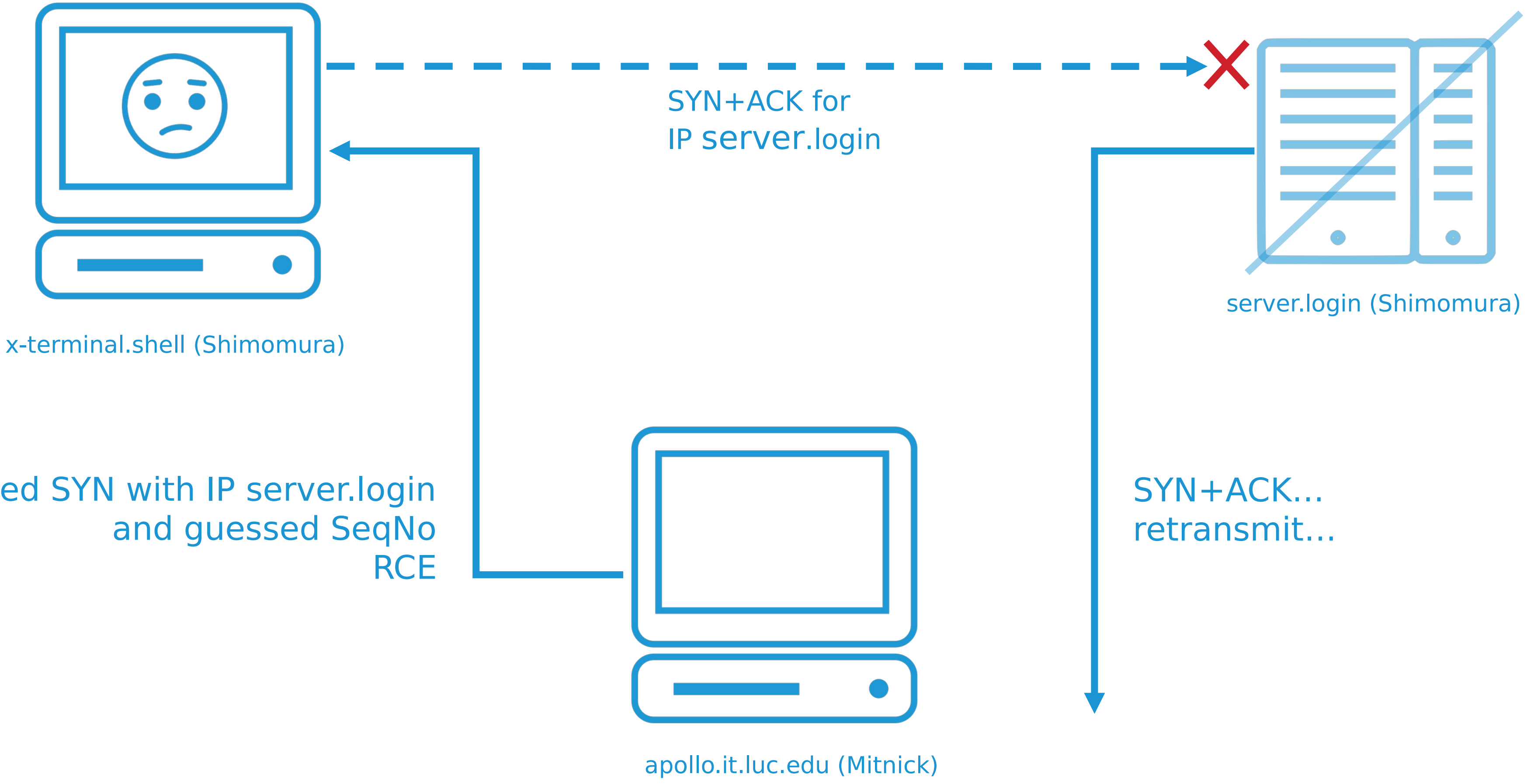
Credit: Icons made from http://www.onlinewebfonts.com/icon is licensed by CC BY 3.0

1994: Mitnick’s , SYN Flood DoS


x-terminal.shell (Shimomura)
server.login (Shimomura)
spoofed SYN with IP
server.login
many SYNs from foreign IP 130.92.6.97
no ACKs
apollo.it.luc.edu (Mitnick)

Credit: Icons made from http://www.onlinewebfonts.com/icon is licensed by CC BY 3.0

1994: Mitnick’s , SYN Flood DoS



SYN+ACK for
IP server.login

x-terminal.shell (Shimomura)

server.login (Shimomura)

spoofed SYN with IP server.login
and guessed SeqNo
RCE

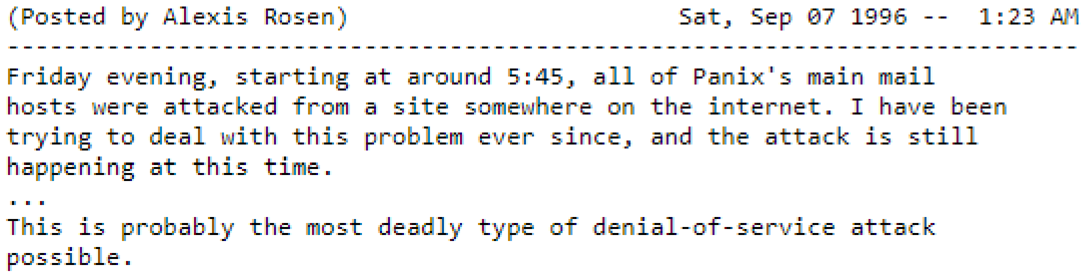
SYN+ACK...
retransmit...

apollo.it.luc.edu (Mitnick)

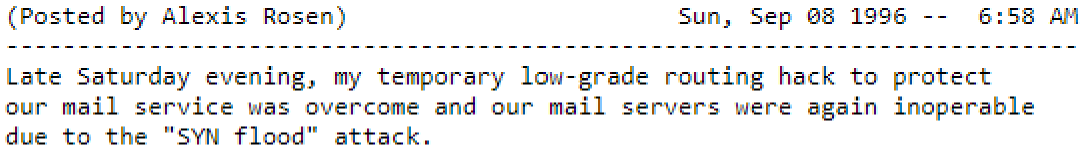
Credit: Icons made from http://www.onlinewebfonts.com/icon is licensed by CC BY 3.0

1996–2010: Occurrence and Development of Basic Methods

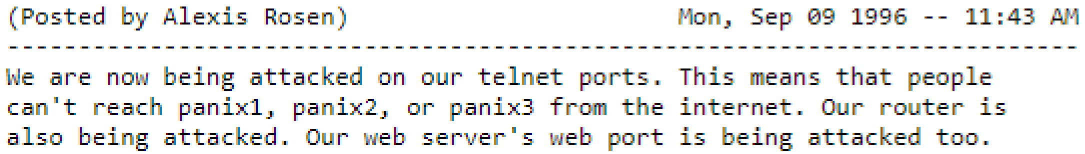
1996: PANIX SYN Flood



```
(Posted by Alexis Rosen)                              Sat, Sep 07 1996 --  1:23 AM
----------------------------------------------------------------------------
Friday evening, starting at around 5:45, all of Panix's main mail
hosts were attacked from a site somewhere on the internet. I have been
trying to deal with this problem ever since, and the attack is still
happening at this time.
...
This is probably the most deadly type of denial-of-service attack
possible.
```

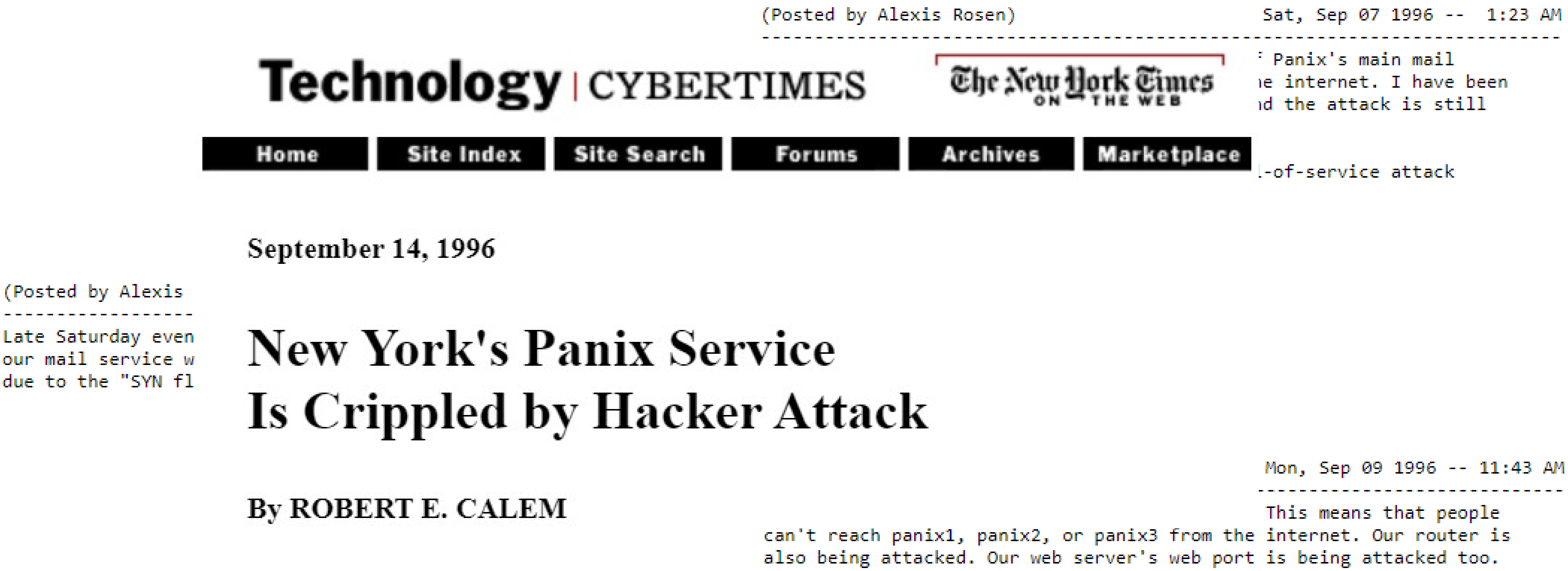


```
(Posted by Alexis Rosen)                              Sun, Sep 08 1996 --  6:58 AM
----------------------------------------------------------------------------
Late Saturday evening, my temporary low-grade routing hack to protect
our mail service was overcome and our mail servers were again inoperable
due to the "SYN flood" attack.
```



```
(Posted by Alexis Rosen)                              Mon, Sep 09 1996 -- 11:43 AM
----------------------------------------------------------------------------
We are now being attacked on our telnet ports. This means that people
can't reach panix1, panix2, or panix3 from the internet. Our router is
also being attacked. Our web server's web port is being attacked too.
```

1996: PANIX SYN Flood



(Posted by Alexis Rosen) Sat, Sep 07 1996 -- 1:23 AM

Panix's main mail
e internet. I have been
d the attack is still

-of-service attack

Technology | CYBERTIMES

The New York Times ON THE WEB

September 14, 1996

New York's Panix Service Is Crippled by Hacker Attack

By ROBERT E. CALEM

(Posted by Alexis

Late Saturday even
our mail service w
due to the "SYN fl

Mon, Sep 09 1996 -- 11:43 AM

This means that people
can't reach panix1, panix2, or panix3 from the internet. Our router is
also being attacked. Our web server's web port is being attacked too.

Source: New York Times

1996: PANIX SYN Flood – Reaction

«20pps is enough to keep the SYN queue full» Internet Protocols for Network-Attached Peripherals Steve Hotz, Rodney Van Meter, and Gregory Finn, Information Sciences Institute University of Southern California, 1998

«ISPs: Filter spoofed IP traffic through your networks» CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks

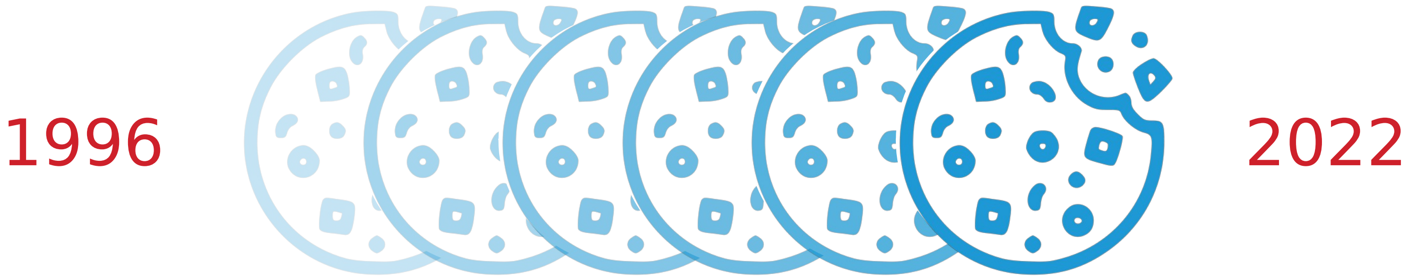
SYN cookies: idea 7 days after attack, implementation - 1 month later Daniel J. Bernstein, Eric Schenk

1996: PANIX SYN Flood – Reaction

«20pps is enough to keep the SYN queue full» Internet Protocols for Network-Attached Peripherals Steve Hotz, Rodney Van Meter, and Gregory Finn, Information Sciences Institute University of Southern California, 1998

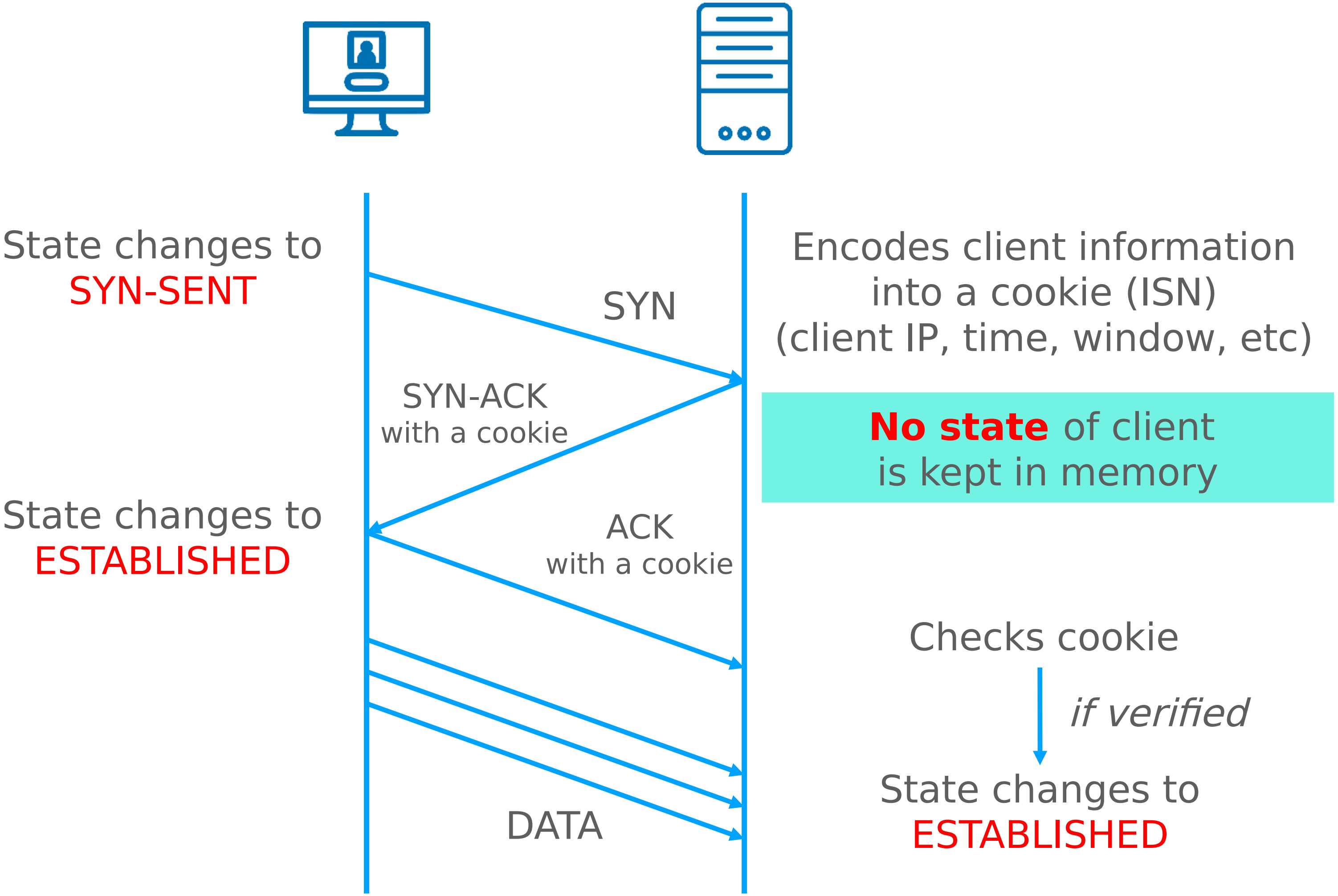
«ISPs: Filter spoofed IP traffic through your networks» CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks

SYN cookies: idea 7 days after attack, implementation - 1 month later Daniel J. Bernstein, Eric Schenk



Credit: Icons made from http://www.onlinewebfonts.com/icon is licensed by CC BY 3.0

Mechanism of SYN-Cookies



State changes to
SYN-SENT

SYN

Encodes client information
into a cookie (ISN)
(client IP, time, window, etc)

SYN-ACK
with a cookie

No state of client
is kept in memory

State changes to
ESTABLISHED

ACK
with a cookie

Checks cookie

if verified

State changes to
ESTABLISHED

DATA

https://datatracker.ietf.org/doc/html/rfc6013

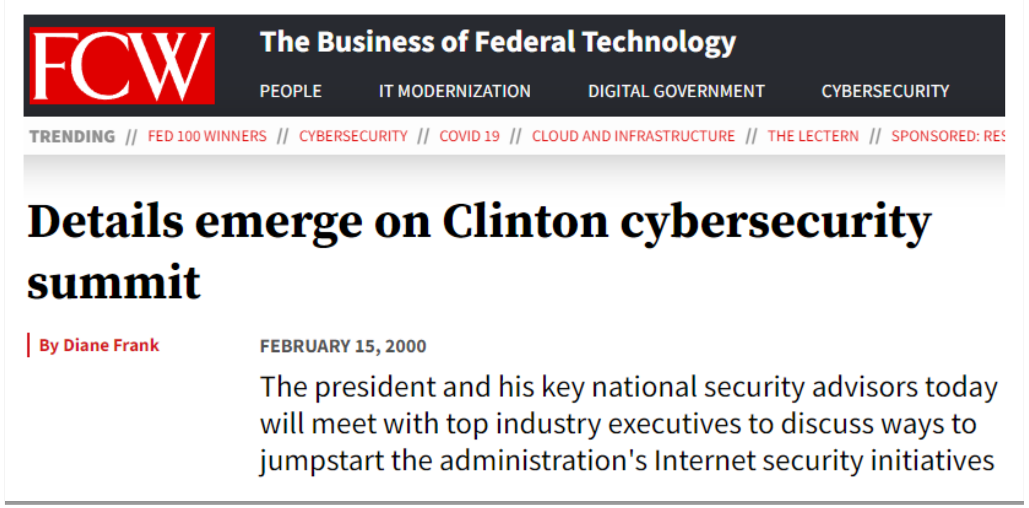
2000: MafiaBoy Shuts Down Top Sites

ebaY
amazon.com
Buy.com
YAHOO!

1-2 attack/day, 8 days’ duration
~800Mbps (Buy.com) attack bandwidth
university hosts traffic sources

Source: Google

2000: MafiaBoy Shuts Down Top Sites



FCW The Business of Federal Technology

PEOPLE IT MODERNIZATION DIGITAL GOVERNMENT CYBERSECURITY

TRENDING // FED 100 WINNERS // CYBERSECURITY // COVID 19 // CLOUD AND INFRASTRUCTURE // THE LECTERN // SPONSORED: RES

Details emerge on Clinton cybersecurity summit

By Diane Frank

FEBRUARY 15, 2000

The president and his key national security advisors today will meet with top industry executives to discuss ways to jumpstart the administration's Internet security initiatives

1-2 attack/day, 8 days’ duration

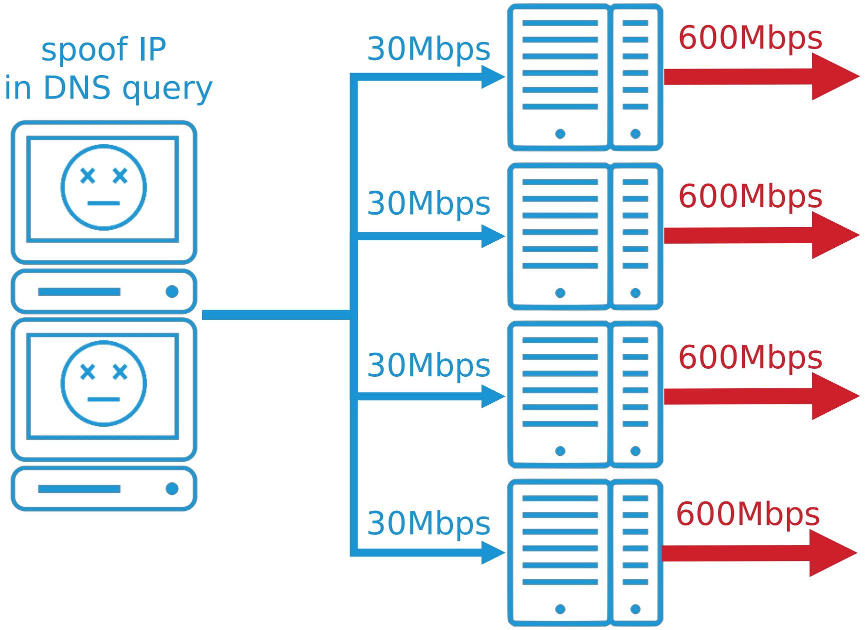
~800Mbps (Buy.com) attack bandwidth

university hosts traffic sources

Source: Google

2006: Amplification Attacks

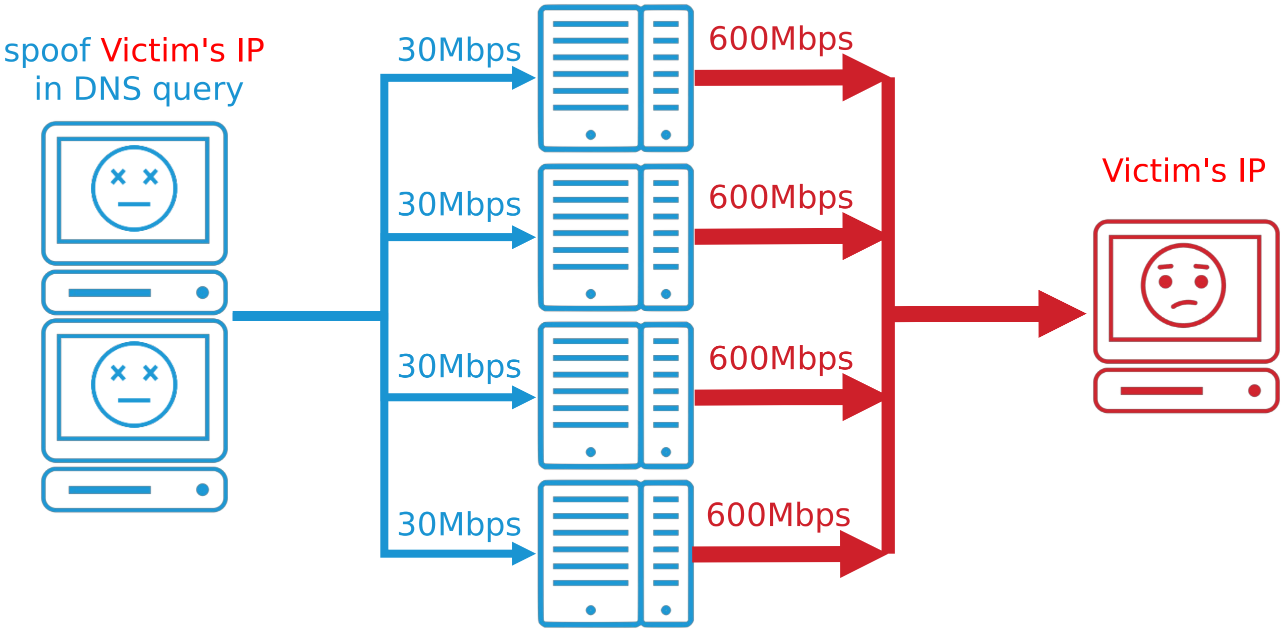
The Continuing DoS Threat Posed by DNS Recursion, US CERT 2005
2.4Gbps peak, 14 minutes attack on TLD



Credit: Icons made from http://www.onlinewebfonts.com/icon is licensed by CC BY 3.0

2006: Amplification Attacks

The Continuing DoS Threat Posed by DNS Recursion, US CERT 2005
2.4Gbps peak, 14 minutes attack on TLD

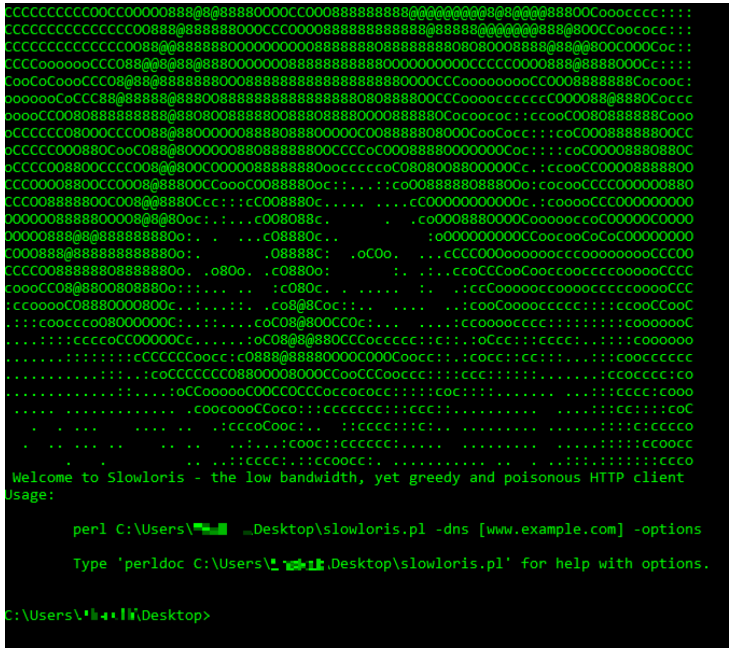


Credit: Icons made from http://www.onlinewebfonts.com/icon is licensed by CC BY 3.0

2007–2010: DDoS Hacktivism

TCP/UDP flood

HTTP GET/POST flood



```
 Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client
Usage:

        perl C:\Users\[redacted]Desktop\slowloris.pl -dns [www.example.com] -options

        Type 'perldoc C:\Users\[redacted]Desktop\slowloris.pl' for help with options.


C:\Users\[redacted]\Desktop>
```

Slow HTTP headers

Source: Wikimedia

2010–2016: Attacks on Sony. Spamhaus. The Evolution of Protection Methods

1994

We’re here

2022

2011–2014: Troubles of Sony

Source: Daily Mirror

2011–2014: Troubles of Sony

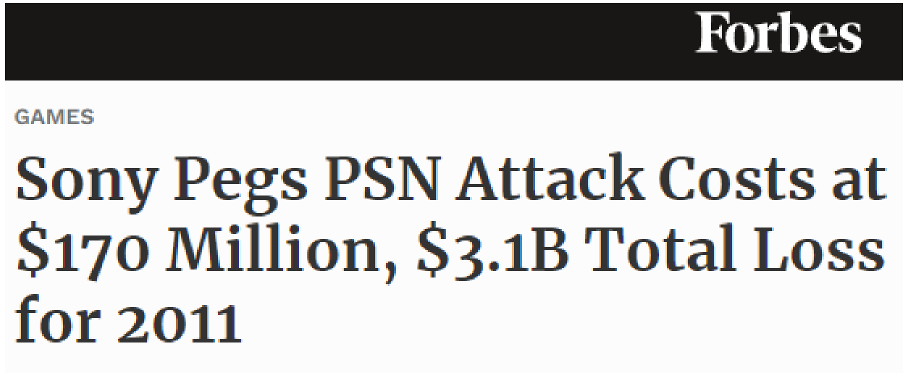
2011: hacking under the cover of a DDoS attack

annual attacks on the PlayStation Network

2014: hacking under the cover of a DDoS attack

hacked routers as part of a botnet

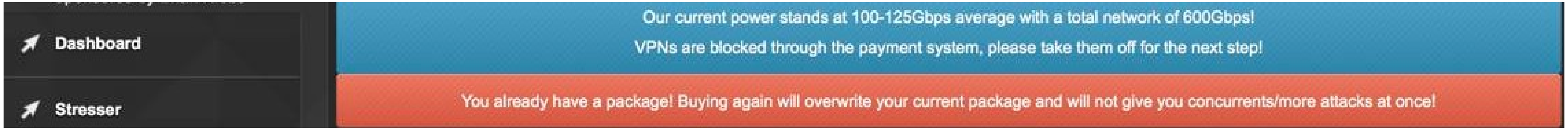
~100..125Gbps possible attack’s bandwidth



Forbes

GAMES

Sony Pegs PSN Attack Costs at $170 Million, $3.1B Total Loss for 2011



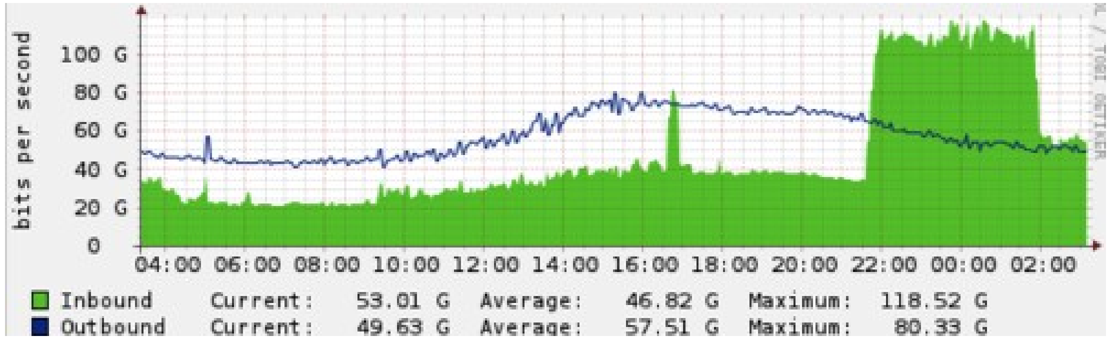
Our current power stands at 100-125Gbps average with a total network of 600Gbps!

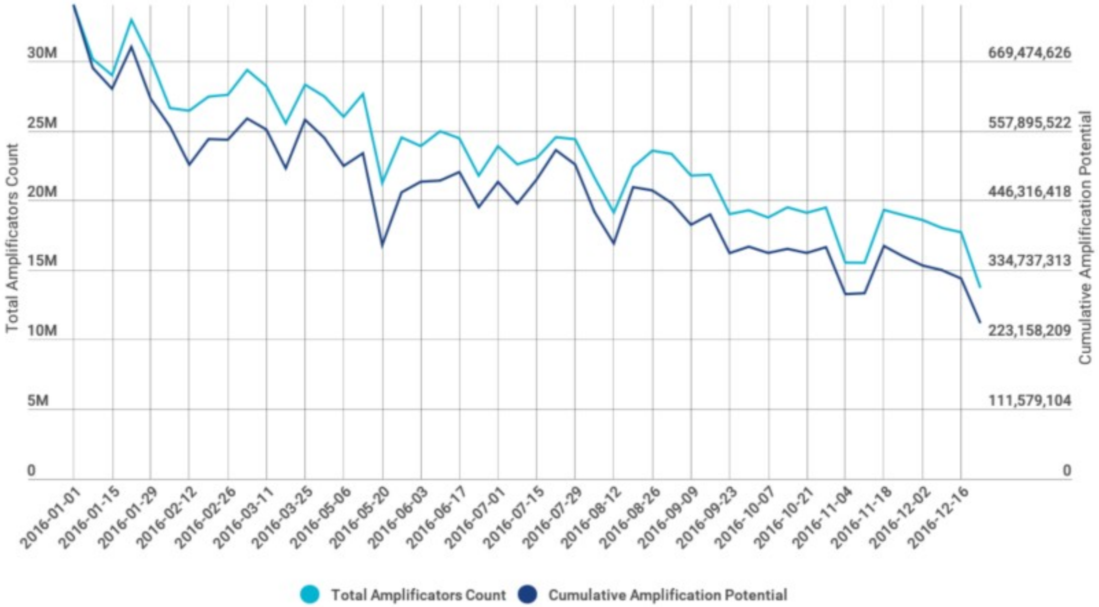
VPNs are blocked through the payment system, please take them off for the next step!

You already have a package! Buying again will overwrite your current package and will not give you concurrents/more attacks at once!

Source: **Forbes, Krebs On Security**

2013: Attacks on Spamhaus





75..90Gbps first attack's bandwidth

~300Gbps maximum bandwidth

DNS Amplification method

Source: **Cloudflare, Qrator.Radar Network Scanner**

2010–2016: Development of Protection Services

Customer **On-Premises** Equipment

Protection at ISP

Distributed Filtering Networks

2016–2018: Mirai. Terabit Attacks. Buter Services

1994

We’re here

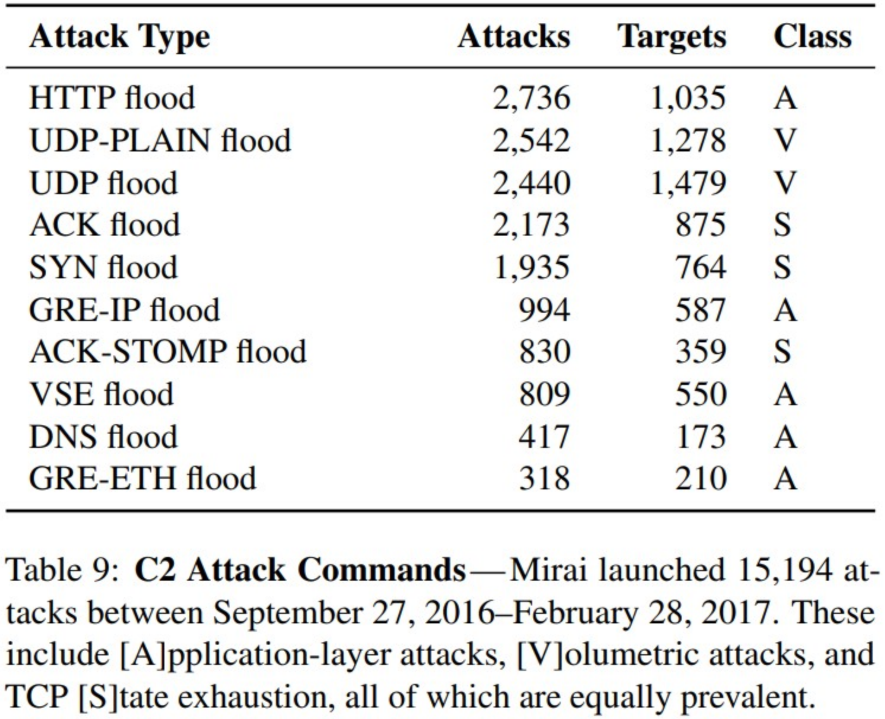
2022

2016: Mirai and "DDoS from the Kettle"

20.09 KrebsOnSecurity

620Gbps bandwidth

~145K bots’ count



Attack Type	Attacks	Targets	Class
HTTP flood	2,736	1,035	A
UDP-PLAIN flood	2,542	1,278	V
UDP flood	2,440	1,479	V
ACK flood	2,173	875	S
SYN flood	1,935	764	S
GRE-IP flood	994	587	A
ACK-STOMP flood	830	359	S
VSE flood	809	550	A
DNS flood	417	173	A
GRE-ETH flood	318	210	A

Table 9: **C2 Attack Commands**—Mirai launched 15,194 attacks between September 27, 2016–February 28, 2017. These include [A]pplication-layer attacks, [V]olumetric attacks, and TCP [S]tate exhaustion, all of which are equally prevalent.

Source: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

2016: Mirai and "DDoS from the Kettle"

20.09 KrebsOnSecurity

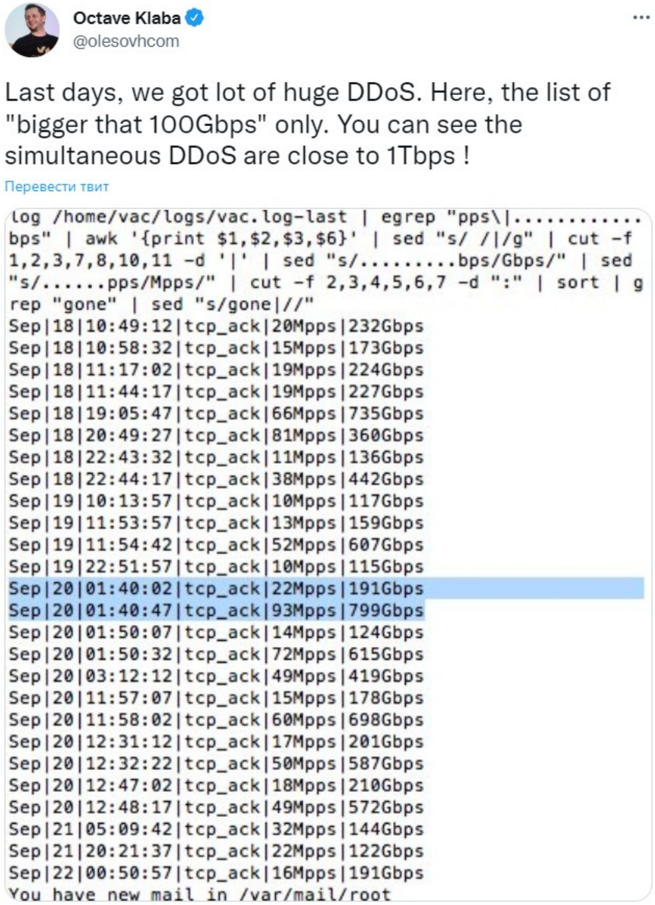
620Gbps bandwidth

~145K bots’ count

20.09 OVH

~990Gbps bandwidth

21.10 Dyn ?

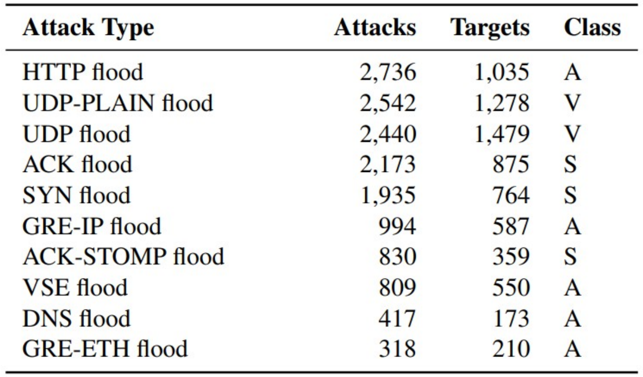


Octave Klaba
@olesovhcom

Last days, we got lot of huge DDoS. Here, the list of "bigger that 100Gbps" only. You can see the simultaneous DDoS are close to 1Tbps !

Перевести твит

```
log /home/vac/logs/vac.log-last | egrep "pps\|............
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.........bps/Gbps/" | sed
"s/......pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|//"
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps
Sep|20|11:58:02|tcp_ack|60Mpps|698Gbps
Sep|20|12:31:12|tcp_ack|17Mpps|201Gbps
Sep|20|12:32:22|tcp_ack|50Mpps|587Gbps
Sep|20|12:47:02|tcp_ack|18Mpps|210Gbps
Sep|20|12:48:17|tcp_ack|49Mpps|572Gbps
Sep|21|05:09:42|tcp_ack|32Mpps|144Gbps
Sep|21|20:21:37|tcp_ack|22Mpps|122Gbps
Sep|22|00:50:57|tcp_ack|16Mpps|191Gbps
You have new mail in /var/mail/root
```

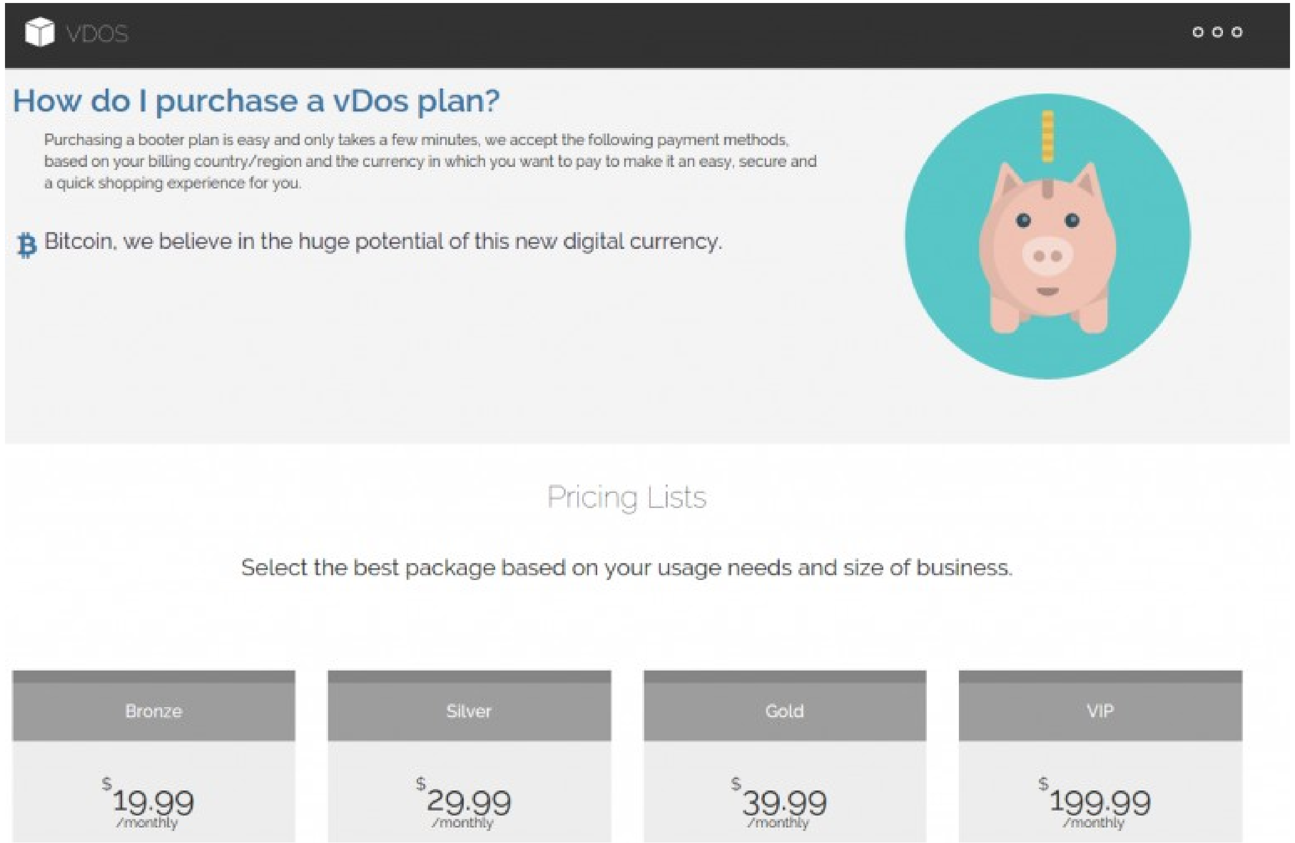


Attack Type	Attacks	Targets	Class
HTTP flood	2,736	1,035	A
UDP-PLAIN flood	2,542	1,278	V
UDP flood	2,440	1,479	V
ACK flood	2,173	875	S
SYN flood	1,935	764	S
GRE-IP flood	994	587	A
ACK-STOMP flood	830	359	S
VSE flood	809	550	A
DNS flood	417	173	A
GRE-ETH flood	318	210	A

Table 9: **C2 Attack Commands**—Mirai launched 15,194 attacks between September 27, 2016–February 28, 2017. These include [A]pplication-layer attacks, [V]olumetric attacks, and TCP [S]tate exhaustion, all of which are equally prevalent.

Source: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

2016: DDoS as a service? Yes, long ago.



VDOS

How do I purchase a vDos plan?

Purchasing a booter plan is easy and only takes a few minutes, we accept the following payment methods, based on your billing country/region and the currency in which you want to pay to make it an easy, secure and a quick shopping experience for you.

₿ Bitcoin, we believe in the huge potential of this new digital currency.

Pricing Lists

Select the best package based on your usage needs and size of business.

Bronze	Silver	Gold	VIP
$19.99 /monthly	$29.99 /monthly	$39.99 /monthly	$199.99 /monthly

Source: are you serious?!

2018– : Memcached, Hybrids, Mēris, New Protocols

1994

We’re here

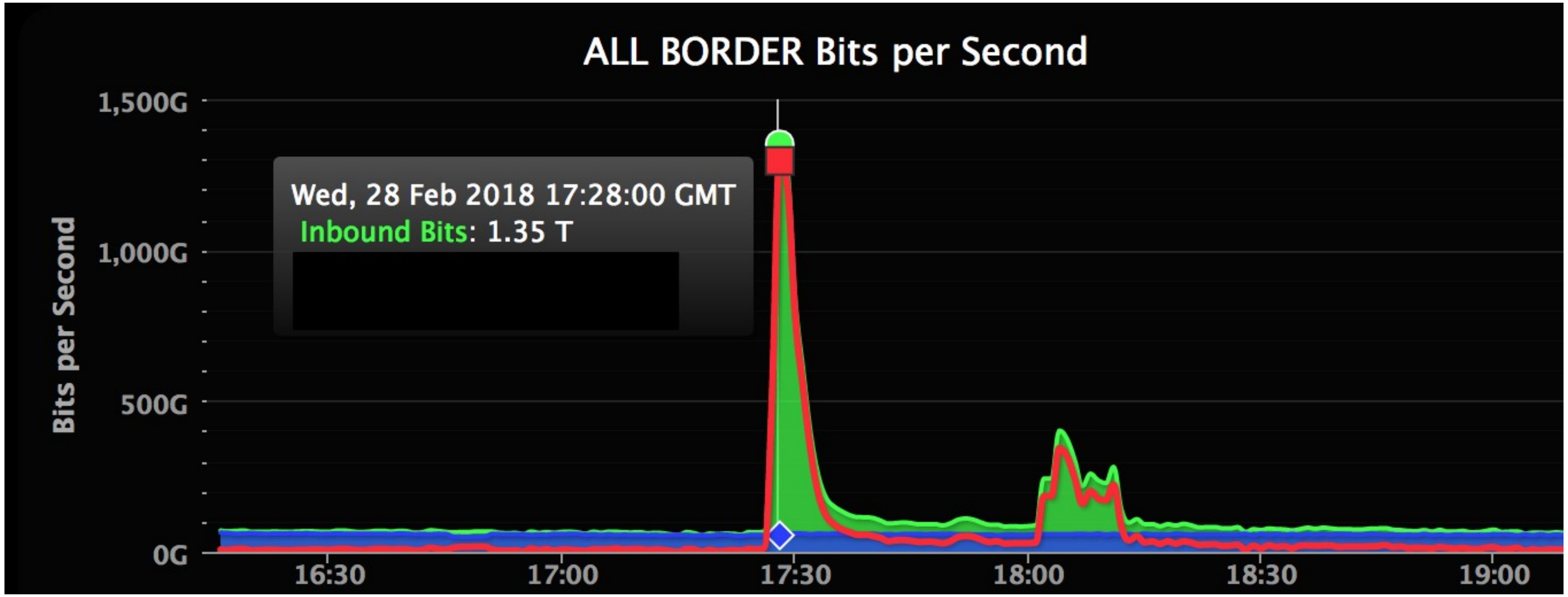
2022

2018: Memcached Amplification

1,35Tbps bandwidth

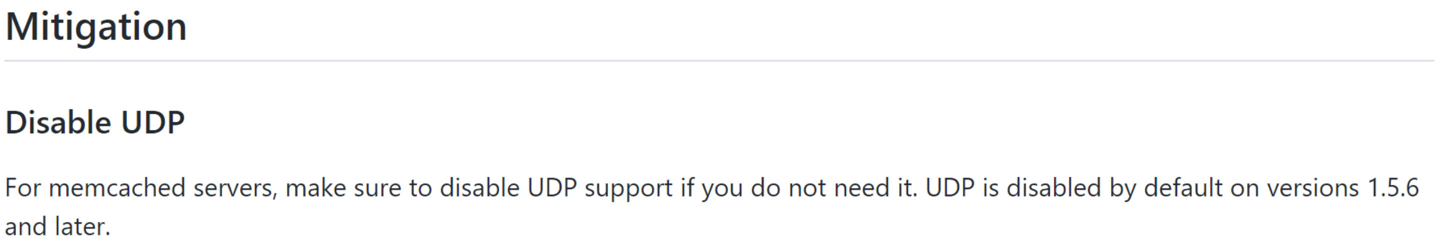
8 минут downtime

~91000 open servers by Shodan



Source: Github

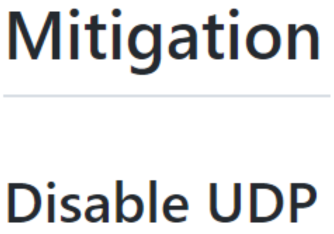
2018: Memcached Amplification



Mitigation

Disable UDP

For memcached servers, make sure to disable UDP support if you do not need it. UDP is disabled by default on versions 1.5.6 and later.



Mitigation

Disable UDP

Disable UDP

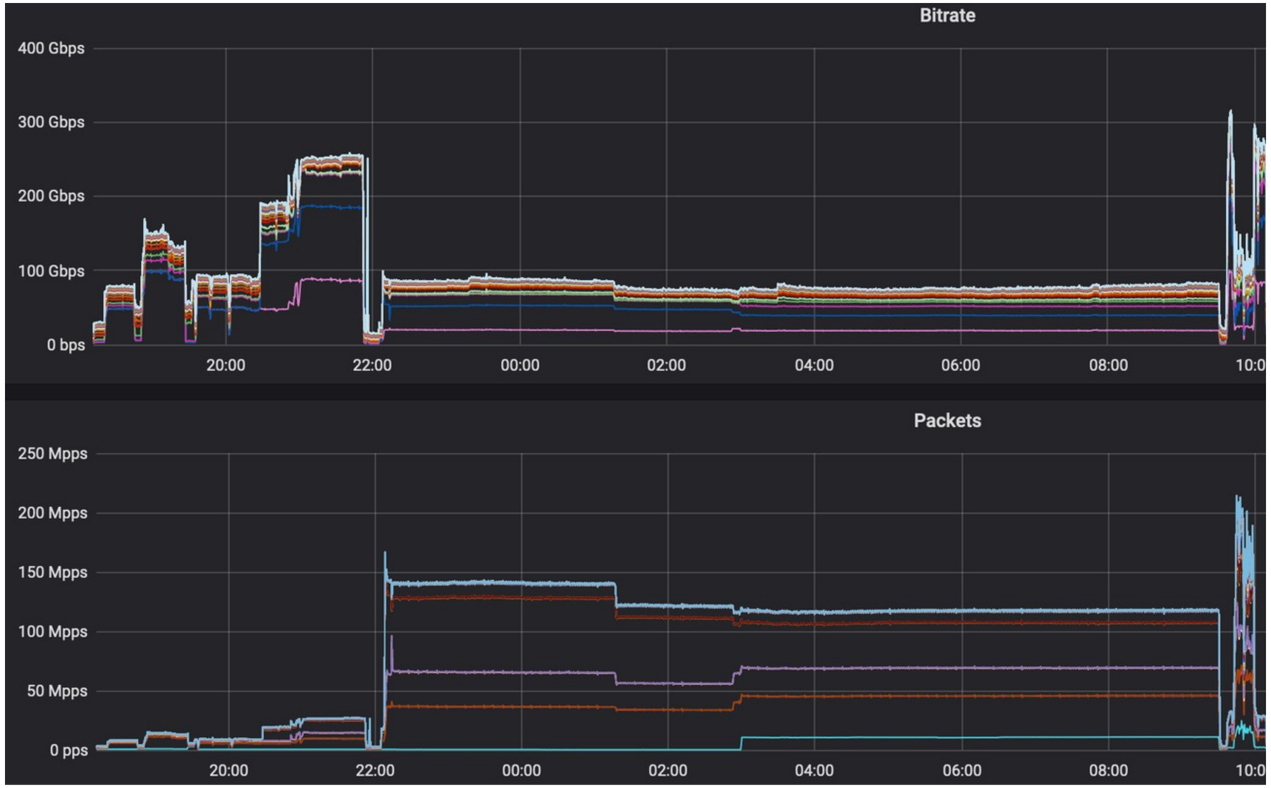
Source: Github

2019: TCP SYN-ACK Amplification

300+Gbps bandwidth

215+Mpps packets

12 hours' duration

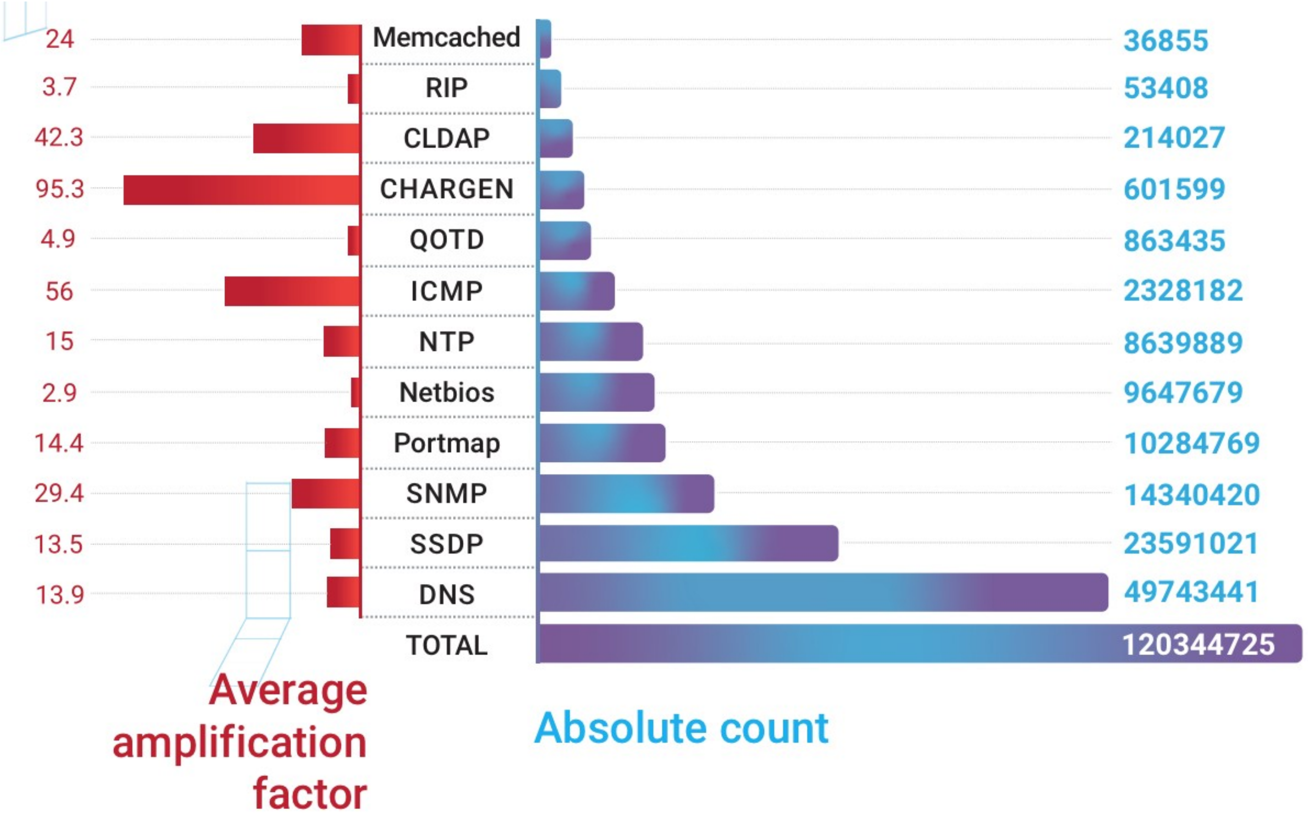


Source: **S**ervers.com, Qrator

2019: TCP SYN-ACK Amplification

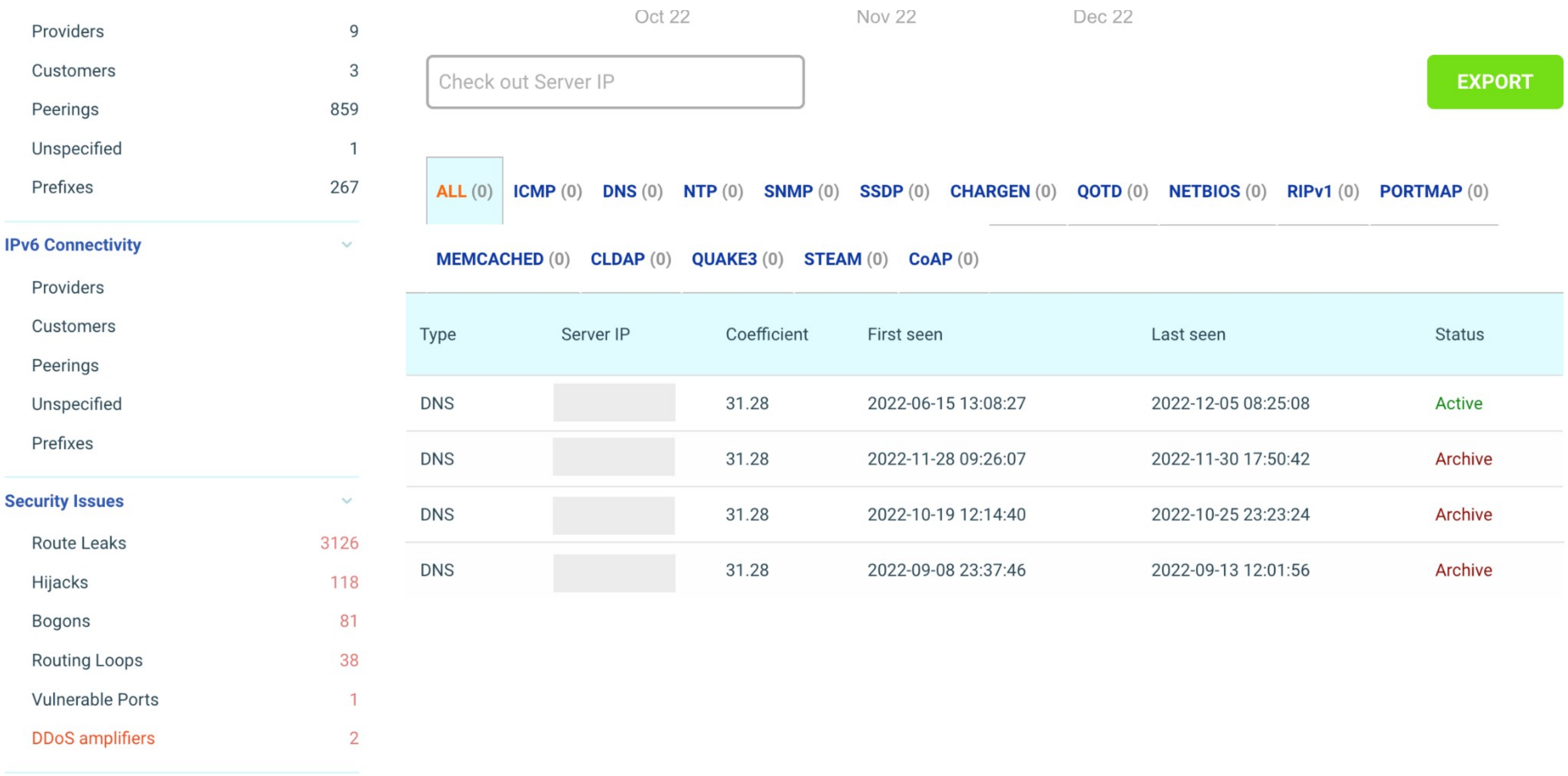
3-5x amplification factor

10^7 potential count of amplifiers



Source: Qrator

2019: Amplifiers’ Check



Providers	9
Customers	3
Peerings	859
Unspecified	1
Prefixes	267

IPv6 Connectivity

- Providers
- Customers
- Peerings
- Unspecified
- Prefixes

Security Issues

Route Leaks	3126
Hijacks	118
Bogons	81
Routing Loops	38
Vulnerable Ports	1
DDoS amplifiers	2

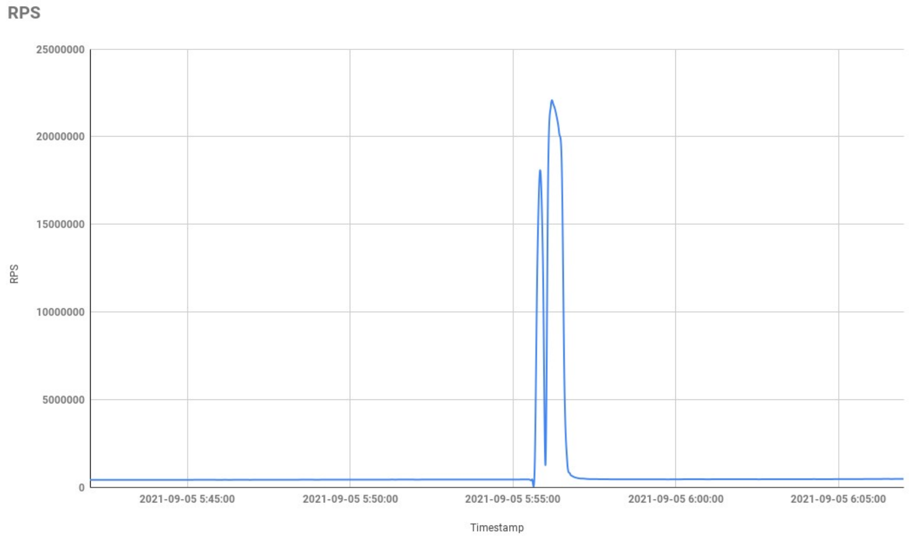
Type	Server IP	Coefficient	First seen	Last seen	Status
DNS	[redacted]	31.28	2022-06-15 13:08:27	2022-12-05 08:25:08	Active
DNS	[redacted]	31.28	2022-11-28 09:26:07	2022-11-30 17:50:42	Archive
DNS	[redacted]	31.28	2022-10-19 12:14:40	2022-10-25 23:23:24	Archive
DNS	[redacted]	31.28	2022-09-08 23:37:46	2022-09-13 12:01:56	Archive

Source: https://radar.qrator.net

2021: Mēris on MikroTik Routers

21,8Mrps Yandex 2021

17,6Mrps Cloudflare 2021



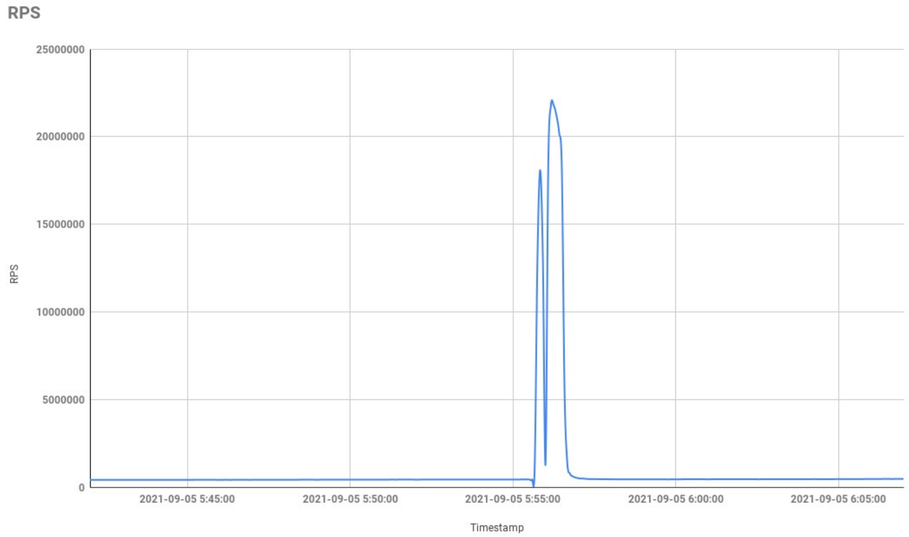
Source: **Yandex**

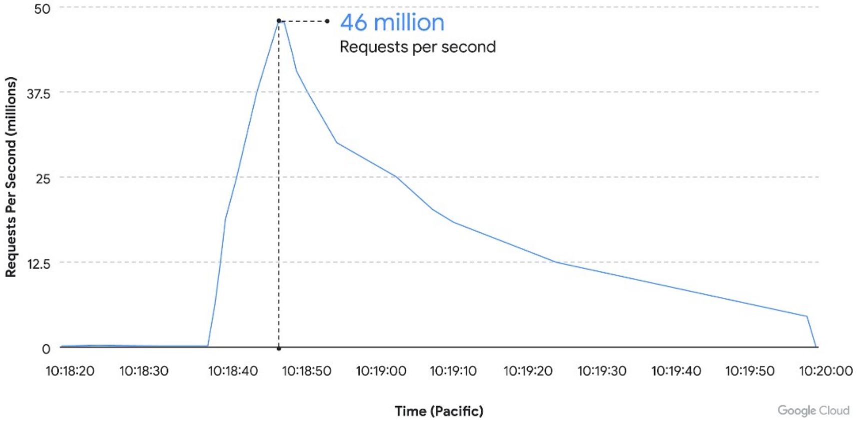
2021: Mēris on MikroTik Routers

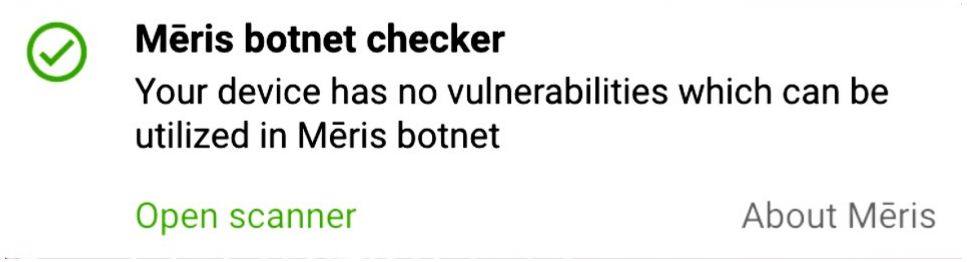
21,8Mrps Yandex 2021

17,6Mrps Cloudflare 2021

46Mrps   Google 2022







Mēris botnet checker

Your device has no vulnerabilities which can be utilized in Mēris botnet

Source: **Yandex, Google Cloud, Qrator.Radar**

New Protocols– New Challenges

2017 H2DoS Xiang Ling, Chunming Wu, Shouling Ji, Meng Han

2017 HTTP/2 Tsunami: Investigating HTTP/2 proxy amplification DDoS attacks
David Beckett, Sakir Sezer

2019 CVE-2019-9511..9518 Netflix security bulletin [1]

[1] https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-002.md

New Protocols– New Challenges

2017 H2DoS Xiang Ling, Chunming Wu, Shouling Ji, Meng Han

2017 HTTP/2 Tsunami: Investigating HTTP/2 proxy amplification DDoS attacks
David Beckett, Sakir Sezer

2019 CVE-2019-9511..9518 Netflix security bulletin [1]

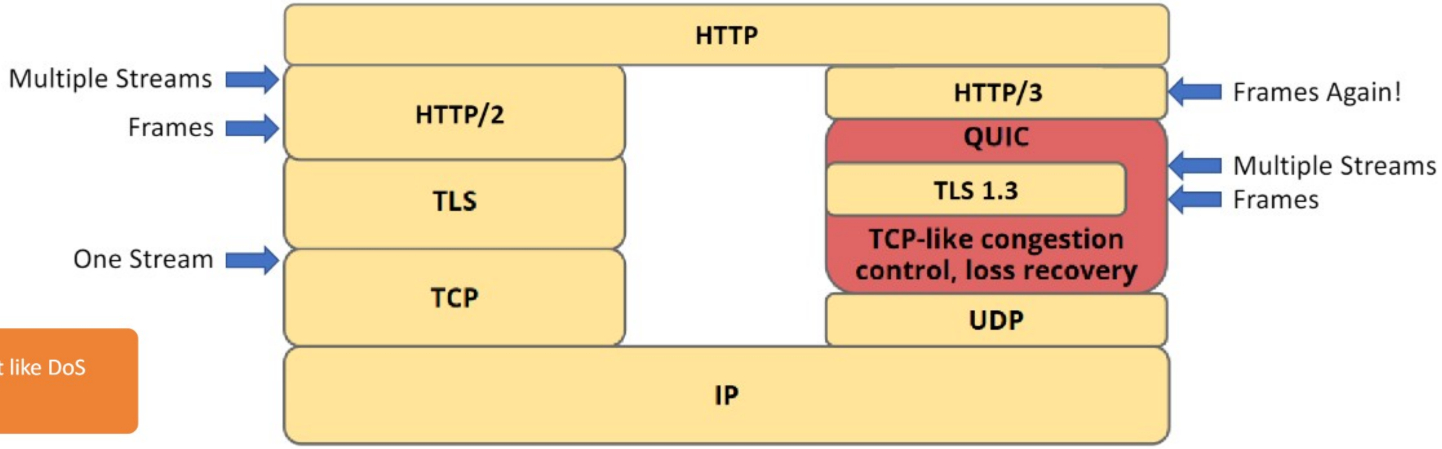
multiplexing

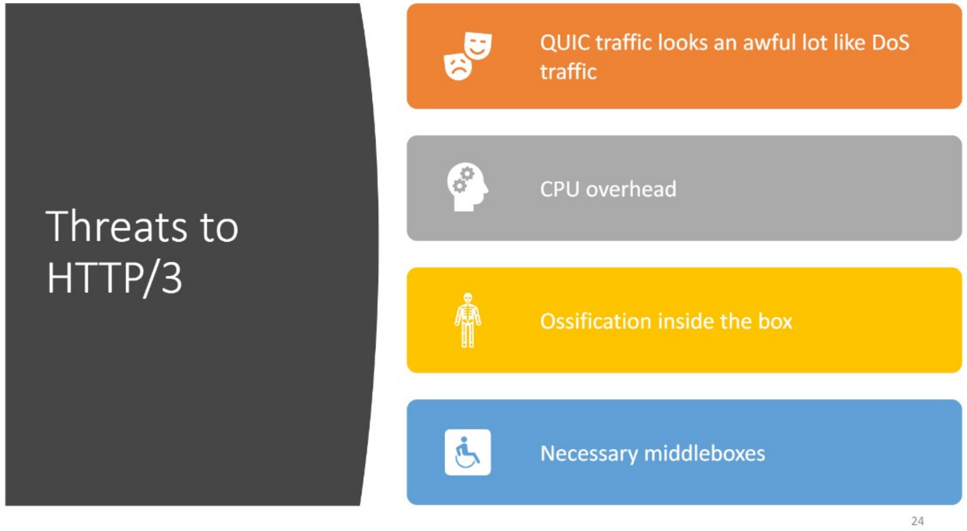
constantly opened connections

compressing headers

[1] https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-002.md

New Protocols– New Challenges



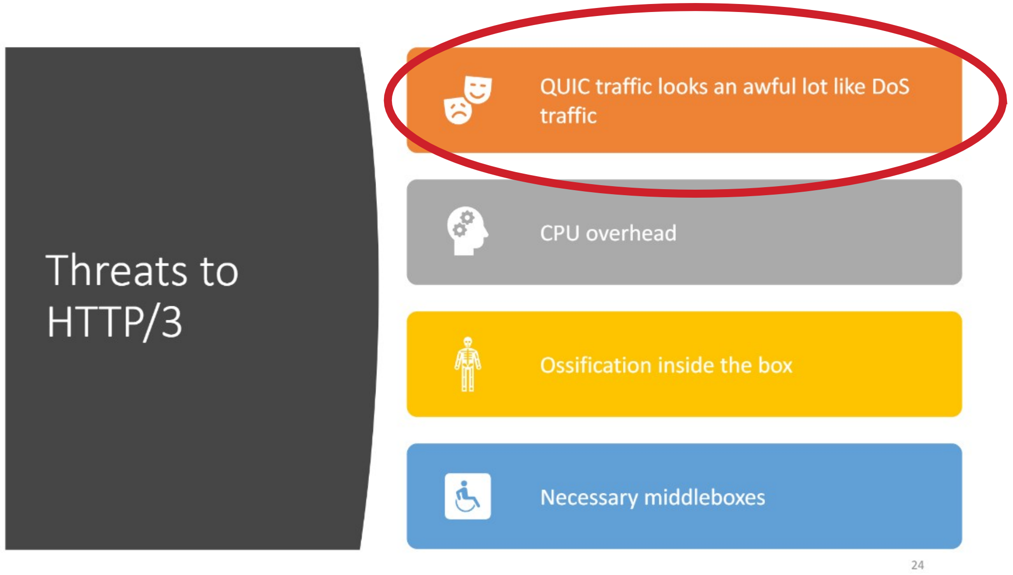


Threats to HTTP/3

- QUIC traffic looks an awful lot like DoS traffic
- CPU overhead
- Ossification inside the box
- Necessary middleboxes

Source: Mike Bishop, Akamai https://github.com/HTTPWorkshop/workshop2019/blob/main/talks/bishop-HTTP3-Thinking.pdf

New Protocols– New Challenges



Threats to HTTP/3

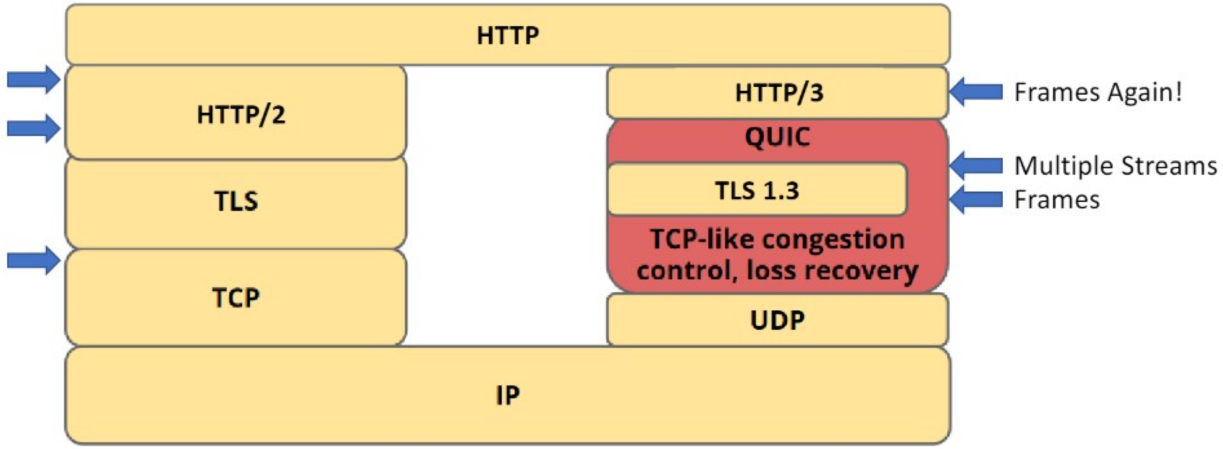
QUIC traffic looks an awful lot like DoS traffic

CPU overhead

Ossification inside the box

Necessary middleboxes

24



Source: Mike Bishop, Akamai https://github.com/HTTPWorkshop/workshop2019/blob/main/talks/bishop-HTTP3-Thinking.pdf

Source: Youtube

What did we understand?

new methods come,
the old ones do not go away.

Most DDoS methods will not be "fixed" without changes in protocols, and this is decades.

Recommendations do not help,
unlike the proactive measures.

Improving the quality of life making the "quality" of attacks better

Credit: Icons made from http://www.onlinewebfonts.com/icon is licensed by CC BY 3.0

Leave your feedback!

You can rate the talk and give feedback on what you've liked or what could be improved

я

Thank you for attention!

✈ @emikayelyan

✉ edgar@qrator.net

++ High Load Armenia

Co-organizer

Yandex